REMARKS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 USC § 103. Furthermore, the Applicants also submit that all of these claims now satisfy the requirements of 35 USC § 112. Thus, the Applicants believe that all of these claims are now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 530-6671 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Specification and abstract amendments

Various amendments have been made to the specification and abstract to correct minor inadvertent grammatical, spelling and formal errors.

In addition, various section headings have now been inserted into the specification.

To facilitate entry of all these amendments, the Applicants have enclosed herewith a marked-up copy of their specification showing these changes and a substitute specification that incorporates all these changes. No new matter has been added to the specification. A replacement Abstract is also submitted.

Status of claims

To conform their claims to the dictates of proper US claim practice, the Applicants, in light of the separate amendments that would need to have been made to their claims, have instead simply chosen to cancel their existing claims and replace them with new claims 15-24.

Claims 15, 18, 19, 21, 22, 23 and 24 respectively and substantively correspond to prior claims 8, 9, 10, 11, 12, 13 and 14, respectively. Claim 17 contains a recitation similar to that which previously appeared in now canceled claim 8.

Rejections

A. Rejections under 35 USC § 112

The Examiner rejected claims 8-14, under the provisions of the second paragraph of 35 USC § 112, as being indefinite.

Specifically, the Examiner noted that, in claim 8, each of the phrases "such as" and "and the like" rendered that claim indefinite.

Corresponding new independent claim 15 does not contain either of these phrases.

Hence, the Applicants submit that all their claims, as they now stand, are sufficiently definite and thus are patentable under the provisions of 35 USC § 112.

B. Rejections under 35 USC § 103

1. Claims 8 and 14

The Examiner rejected independent claim 8 and dependent claim 14, under the provisions of 35 USC § 103, as being obvious over the teachings in the Moroney et al patent (United States patent 5,054,067 issued to P. Moroney et al on October 1, 1991) in view of the Kocher et al patent (United States patent 6,327,661 issued to P. C. Kocher et al on December 4, 2001). Inasmuch as claims 8 and 14 have now been canceled, this rejection is moot. Nevertheless, since claims 8 and 14 have been replaced by new claims 15 and 24, respectively, then, to expedite prosecution, this rejection will be discussed in the context of these two new claims. In that context, this rejection is respectfully traversed.

Specifically, the Examiner take the position that the Moroney et al patent substantially teaches loading plaintext and an encryption key into both linear and non-linear feedback shift registers to produce a pseudorandom non-linear sequence. However, the Examiner concedes that this patent fails to teach use of this method as it would apply to protecting a smart card from attack. Given that failing, the Examiner then turns to the Kocher et al patent for its teachings of a method wherein a pseudo-random number generator is used in a smart card to implement clock-skipping and thus protect that card from attack. With these teachings in mind, the Examiner concludes that it would have been obvious for one of ordinary skill in the art to utilize the pseudo-random number generator disclosed by the Moroney et al patent, apparently within the system

taught by the Kocher et al patent, to increase the "randomness of the pseudo-random generator" and thus the security of the system as a whole, and, by so doing, arrive at the Applicants' present invention.

While the Examiner is certainly correct in her specific observations as to what the Moroney et al and Kocher et al patents disclose, combining these teachings will clearly not render the present invention, as recited in claim 15, obvious.

The Moroney et al patent discloses a block-cipher cryptographic device which utilizes a shift register and processes plaintext/encrypted input data with a key signal to provide encrypted/decrypted output data. As discussed in col. 1, lines 19-23, the device provides a sufficiently high degree of encryption security for a range of applications. While the device is not based on the DES (Data Encryption Standard) algorithm to presumably permit its export from the United States, nevertheless the output of the device is compatible with DES.

As shown in FIG. 1 and discussed in col. 2, line 16 et seq, the device processes an N-byte block of plaintext input data 13 with M-byte encryption key 14 signal to provide an N-byte block of encrypted output data 15. Encryption is performed through use of N-byte feedback shift register 10 -- into which input data 13 is fed, data processing system 12 and adder 44. Based on the M most significant bytes 16 in shift register 10 and on M-byte encryption key 14, data processing system 12 generates single output byte 40. FIG. 1A illustrates the

process performed by system 12. As shown, this process relies on using a hardware-implemented DFAST keystream generator 32. As noted in col. 2, line 61 et seq, this generator uses dynamic feedback arrangement scrambling and with specifically both dynamic (non-linear) and a static (linear) feedback shift registers for receiving data. In operation and within generator 32, the most significant bytes of N bytes 28 are received in the non-linear feedback register and the remaining bytes of N bytes 28 are received in the linear feedback shift register. Given these inputs, DFAST generator 32 then provides high-speed pseudo-random non-linear sequence processing of N bytes 28 to generate keystream 34. A single byte 40 is segregated from the resulting keystream and used to create data that is fed back, via exclusive OR operation 44 (see FIG. 1), for processing in the next iteration (cycle). Exclusive OR operation 44 combines byte 40 with the least significant byte in shift register 10 and applies the resulting byte as input to this shift register as its most significant byte 46. After a selected number of such iterations has completed, then, as stated in col. 4, line 35 et seq, encrypted data 15 is provided as output from shift register 10.

The Examiner is quite correct in observing that the Moroney et al patent contains no teachings whatsoever directed to protecting a smart card from an external attack, let alone from threats pertinent to the present invention and which specifically result from a statistical analysis of "leakage data" from the card, i.e., measurements of power consumed by the card or electromagnetic radiation produced

by the card. The present invention advantageously deters these threats.

The Kocher et al patent, like the present invention, addresses a need to protect a smart card from external attacks and particularly from the same "data leakage" threats that the Applicants address. In that regard, this patent provides low-cost countermeasures that can be incorporated into a smart card and other highly constrained environments where traditional techniques of shielding or other protective measures can not be readily used.

In particular, the Kocher et al patent teaches the concept of decreasing a signal-to-noise (S/N) ratio of the leakage data by incorporating unpredictable and basically random information, i.e., which essentially implements noise, into the cryptographic processing provided by the card. Increasing the noise content of the leakage data increasingly masks and can hence significantly frustrate the detection of any useful data, such as a key, contained in the leakage data. See, e.g., col. 1, lines 64-65; col. 2, lines 15-20; and col. 3, line 10 to col. 4, line 24 of this patent.

As depicted in FIG. 1 and discussed in col. 4, line 28 et seq, the Kocher et al patent teaches generating analog random noise through randomness source 101 and noise processing module 102, with the resulting noise being digitized and applied to module 105. This module introduces the noise into an attacker's measurements in an effort to frustrate external monitoring attacks. The patent teaches

several approaches through which the noise can injected into the processing provided by the card. One such approach involves clock skipping (also known as "clock decorrelation") through which random clock pulses, that drive a processor within the card, are effectively skipped. This, in turn, effectively de-aligns any leakage data which an attacker might externally measure from the card relative to clock signals applied to the card, hence decorrelating both and increasing the difficulty through which any useful information can be extracted from the measured leakage data. See, e.g., col. 7, lines 6-15 and also, in the same column, particularly lines 36-38. As depicted in FIG. 2 and discussed in col. 6, line 18 et seq, random number generator 200 produces a random number at random output 205 which is applied, along with external clock 220, to clock skipping module 240. Module 240 uses that number to select which specific clock pulses on the external clock, to skip and hence not apply, as internal clock 260, to core processor 225 and cryptographic accelerator 280. Alternatively, module 240 may use random output 205 either to select closest corresponding clock pulses on the external clock to apply as the internal clock or even as the internal clock signal itself. Through any of these approaches, the processor operates on a clock signal that is not aligned with the external clock.

Now, with these two applied patents in mind, would the combination of their teachings -- as the Examiner postulates -- yield the present invention? No. Why?

Any of the techniques taught the Kocher et al patent, and particularly clock skipping, aim at injecting noise into the cryptographic processing provided by the card. All that the Moroney et al patent would add to these approaches -- which the Examiner readily admits -- would be arguably, at first blush, a more secure random number source, i.e., the DFAST generator 32, which can be used to generate noise. However, upon close examination, it appears that the Kocher et al patent calls, as noted in col. 4, line 53 et seq, for random source 101 to be "truly random" (or otherwise unpredictable) and not just pseudo-random. Such a source is inherently less predictable and thus more secure than any pseudo-random source which clearly includes DFAST generator 32 taught by the Moroney et al patent.

Given that, no person of skill in the art would seriously consider incorporating the teachings of the Moroney et al patent into those of the Kocher et al patent as the results would be less secure, due to some element of inherent predictability, however difficult to discern, in the resulting pseudo-random sequence which injected noise into the on-card cryptographic processing, and hence INFERIOR to those produced by the Kocher et al patent alone. Consequently and quite contrary to the Examiner's view, that person of skill would simply not combine the teachings of these patents as the Examiner purports to do.

Now, assuming, just for the sake of argument, that that person were to make such a combination, there are simply no teachings that would disclose, teach or even suggest, however implicitly, the present invention.

While the present Applicants address the same basic problem as does the Kocher et al patent, the Applicants use an entirely different approach and one that is not taught or even suggested by that patent.

Specifically, and as shown in FIG. 2 and discussed in page 6, line 24 et seq of the present specification (page and line references being to the substitute specification filed herewith), the Applicants rely on using an N-bit shift register 1a with feedback elements 1b and 1c that implement linear and non-linear functions, respectively. Both of these elements are separately controllable and each can be invoked (activated and deactivated) independently of the other. The Applicants teach that, e.g., while either a key or data is loaded into the register and thereafter, these functions can be selectively and sequentially invoked, e.g., one feedback element can be separately clocked for a given period of time to provide feedback to the register while the other element is not with subsequently the latter element then resuming its clocking operations. Alternatively, with respect to the embodiment shown in FIG. 3 and discussed in page 4, line 34 et seq., a fixed key may be loaded into the shift register and then both the linear and non-linear feedback elements activated for a predefined clocking period. During this time, no data is applied to the shift register. Once the clocking is ended, the data can then be applied.

Advantageously, the Applicants have recognized that, by separately and appropriately controlling the use of the linear and non-linear feedback functions, the leakage data can be made sufficiently resistant to statistical

analysis. Accordingly, the present inventive apparatus is relatively simple and economical to implement.

Both the Moroney et al or Kocher et al patents are utterly devoid of any teachings relating to the use of a shift register with separately controllable linear and non-linear feedback elements for providing cryptographic operations or even just any suggestions about such a technique, and let alone controlling those elements in such a manner as to harden leakage data, in a smart card, from external statistical analysis. Accordingly, to the extent any one of skill in the art were to combine the teachings of these patents, such a combination would simply fall <u>far short</u> of the present invention.

New independent claim 15 contains suitable recitations directed at the distinguishing features of the present invention. In particular, this claim recites as follows, with those recitations shown in a bolded typeface:

> "A method for protecting a portable card, provided with a cryptographic algorithm for enciphering data and/or authenticating the card, against deriving a secret key used in the card from statistical analysis of information leaking away from the card to an outside world in the event of cryptographic operations performed by the card, the card being provided with at least a shift register having linear and non-linear feedback functions for implementing cryptographic algorithms, the method comprising the steps of:
>
> loading data to be processed and a secret key into the shift register of the card; and
>
> **controlling the linear and non-linear feedback functions in such a manner that collection of values of recorded leak-information signals is resistant to deriving the secret key through said statistical analysis of the values.**" [emphasis added]

Claim 24 directly depends from independent claim 15 and recites further distinguishing aspects of the present invention.

Accordingly, the Applicants submit that claim 24 is not rendered obvious by the teachings in the Moroney et al and Kocher et al patents for the same exact reasons set forth above regarding claim 15.

As such, the Applicants submit that both claims 15 and 24 are not rendered obvious by the teachings of these two patents and thus are patentable under the provisions of 35 USC § 103.

2. Claims 9, 10 and 13

The Examiner rejected dependent claims 9, 10 and 13, under the provisions of 35 USC § 103, as being obvious over the teachings in the Moroney et al patent in view of the Kocher et al patent, as applied to claim 8, and further in view of the Shimada patent (United States patent 6,278,780 issued to M. Shimada on August 21, 2001). Inasmuch as claims 9, 10 and 13 have all now been canceled, this rejection is also moot. Nevertheless, since claims 9, 10 and 13 have been replaced by new dependent claims 18, 19 and 23, respectively, then, to expedite prosecution, this rejection will be discussed in the context of these three new claims. In that context, this rejection is respectfully traversed.

The Examiner states that the Shimada patent discloses a method where with respect to: (a) claim 9, after

an internal key has been loaded into a shift register, the register clocks on and data bits are loaded; (b) claim 10, after the shift register has been clocked on, the contents of the shift register is filled with the initial key; and (c) claim 13, where internal keys are generated as initial keys and utilized for linear feedback shift registers, and where the contents of the shift register are fixed in that the register is always empty in order for an initial key to be loaded.

The Shimada patent discloses a method for generating, with sufficiently high speed and security, internal keys to be set in feedback shift registers of a pseudo-random sequence generator used in a stream cipher system for use in generating pseudo-random numbers. These numbers, in turn, are combined, through an exclusive-OR operation, with a data sequence with the result either being recorded on a recording medium or transmitted in a communication system. The purpose in using this method is to prevent a third-party from tapping the data sequence without permission.

Specifically, the pseudo-random number generator, shown in FIG. 6 and described in col. 1, line 65 et seq of the Shimada patent -- which appear to be the only teachings in this patent particularly pertinent to the present invention, contains N linear or non-linear feedback shift registers S_1, ..., S_n, each operating as a sub-generator. An internal key from keys K_1,..., K_n is initially applied to each corresponding one of the feedback shift registers. Each such register is then shifted by one bit and provides its least significant bit, as output, to a combination

function F. Each such register generates its most significant bit from its registered bit sequence and according to a certain feedback function. The combination function F generates a key-stream bit-by-bit according to a certain combination function from outputs of feedback shift registers S_1 to S_n.

The Shimada patent, being directed simply to producing a pseudo-random sequence, is also devoid of any teachings relevant to the problem solved by the present Applicants; namely, how to protect a smart card from external attacks arising from statistical analysis of data leakage. All that this patent teaches is a pseudo-random number generator.

Merely incorporating such a generator as taught by the Shimada patent into a system predicated on the teachings of the Moroney et al and Kocher et al patents -- again assuming that the teachings of the latter two patents would in fact be combined by any one of skill in the art, would simply not result in a system that lies any closer to the Applicants' inventive teachings than would a system resulting from just combining the teachings in the Moroney et al and Kocher et al patents. Specifically, such a generator would simply take the place of the DFAST generator disclosed by the Moroney et al patent.

Hence, new independent claim 15 is not rendered obvious over the teachings in these three applied patents, whether taken singly or in any combination -- including that posed by the Examiner, for the same exact reasons set forth

above with respect to the Moroney et al and Kocher et al patents.

Each of claims 18, 19 and 23 depends, either directly or indirectly, from independent claim 15 and recites further distinguishing aspects of the present invention. Consequently, the Applicants submit that each of these three dependent claims is not rendered obvious by the teachings in these references. Consequently, all three of these claims are patentable over these applied references for the same reasons set forth above with respect to claim 15.

3. Claims 11 and 12

The Examiner rejected dependent claims 11 and 12, under the provisions of 35 USC § 103, as being obvious over the teachings in the Moroney et al patent in view of the Kocher et al patent, as applied to claim 8, and further in view of the Rose patent (United States patent 6,510,228 issued to G. G. Rose on January 21, 2003). Inasmuch as claims 11 and 12 have also been canceled, this rejection is also moot. Nevertheless, since claims 11 and 12 have been replaced by new dependent claims 21 and 22, respectively, then, to expedite prosecution, this rejection will be discussed in the context of these two new claims. In that context, this rejection is respectfully traversed.

The Examiner states that the Rose patent discloses a method where with respect to: (a) claim 11, where, during a clocking interval, an output is not generated and hence no new data is loaded into a shift register during or prior to

that clocking; and (b) claim 12, since the input data is not being loaded into the shift register, the data is not connected to that register during that interval.

Specifically, the Rose patent discloses a method and apparatus for generating encryption stream ciphers, and in particular an encryption bit stream for use therein. Here, the bit stream is generated through use of a recurrence relation designed to operate over finite fields larger than a Galois Field of order 2.

A linear feedback register, which can be realized using a circular buffer or sliding window, implements the recurrence relation. See, e.g., col. 2, line 26 et seq of this patent. As noted in col. 3, line 1 et seq, linearity is removed from the output of the shift register through use of one or a combination of various processes: irregular stuttering (also referred to as decimation), a non-linear function, multiple shift registers coupled with combining the outputs of the registers, a variable feedback polynomial on one register, and other non-linear processes. Further and as indicated in col. 3, line 10 et seq, a non-linear output can be derived by performing a non-linear operation on selected elements of the shift register.

For example, in the exemplary embodiment shown in FIG. 4 and as discussed in col. 10, lines 54 et seq, stuttering and a non-linear function are used to remove the linearity of 16-byte shift register 52 from its output. The non-linear function is multiplication (62) of sums formed by modulo 256 adders 60a and 60b to which the values of four specific bytes in the register (S_n and S_{n+5}; and S_{n+2}

and S_{n+12}, respectively) are collectively applied. Since the non-linear output derived from the state of the linear feedback shift register may (still) be used to reconstruct the state of the shift register, stuttering is introduced to render this reconstruction more difficult. Stuttering is performed by not representing some of the states at the output of the generator, and choosing which do so appear but in an unpredictable manner. To implement this, the non-linear output determines what subsequent bytes of the non-linear output appear in the output encryption bit stream. This is accomplished by switch 68, buffer 70, multiplexer 64 and exclusive OR gate 66. See, col. 11, line 60 through col. 12, line 63.

The Rose patent, being directed to a encryption bit stream generator for use in a stream cipher, is also devoid, just like the Shimada patent is, of any teachings relevant to the problem solved by the present Applicants; namely, how to protect a smart card from external attacks arising from statistical analysis of data leakage.

Merely incorporating an encryption bit stream generator as taught by the Rose patent into a system predicated on the teachings of the Moroney et al and Kocher et al patents -- here too assuming that the teachings of the latter two patents would in fact be combined by any one of skill in the art, would simply not result in a system that lies any closer to the Applicants' inventive teachings than would a system resulting from just combining the teachings in the Moroney et al and Kocher et al patents. Specifically, such a bit stream generator, though suitably modified for use in a block cipher, could simply be another

way to generate a keystream and thus could be substituted for the DFAST generator disclosed by the Moroney et al patent.

Hence, new independent claim 15 is not rendered obvious over the teachings in these three applied patents, whether taken singly or in any combination -- including that posed by the Examiner, for the same exact reasons set forth above with respect to the Moroney et al and Kocher et al patents.

Each of claims 21 and 22 depends, either directly or indirectly, from independent claim 15 and recites further distinguishing aspects of the present invention. Consequently, the Applicants submit that each of these two dependent claims is not rendered obvious by the teachings in these references. Hence, both of these claims are patentable over these applied references for the same reasons set forth above with respect to claim 15.

Conclusion

Thus, the Applicants submit that none of the claims, presently in the application, is obvious under the provisions of 35 USC § 103. Furthermore, the Applicants also submit that all of these claims now fully satisfy the requirements of 35 USC § 112.

Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,

November 3, 2005

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer Number: 007265
(732) 530-6671

MICHAELSON AND ASSOCIATES
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **November 4, 2005** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to the Hon. Commissioner for Patents, Mail Stop Non-fee Amendment, P.O. Box 1450, Alexandria, VA 22313-1450.

30,090

Signature — Reg. No.

(PTT128AMEND/ca:160)